INTERNATIONAL MARITIME ORGANIZATION

IMO

E

MARITIME SAFETY COMMITTEE
76th session
Agenda item 4

MSC 76/4/1/Add.1
8 October 2002
Original: ENGLISH

MEASURES TO ENHANCE MARITIME SECURITY

International Code for the Security of Ships and of Port Facilities

Consolidated proposed Part B of the International Maritime Security Code

Note by the Chairman of ISWG and the Secretariat

SUMMARY

Executive summary:	This document provides the revised consolidated text of proposed Part B of the draft ISPS Code prepared by the Chairman of the ISWG and the Secretariat
Action to be taken:	Paragraph 3
Related documents:	MSC 76/4/1

1 MSC 75 noted that, due to time constrains, the Working Group on Maritime Security (MSWG) had not been able to consider and prepare texts for the recommendatory Part B of the draft ISPS Code leaving it as set out in annex 3 to document MSC 75/WP.7.

2 In order to assist the ISWG in its work on the development of that part B of the ISPS Code, the Chairman developed appropriate draft text for consideration by the ISWG in September 2002. The ISWG considered the draft text and a range of amendments thereto were discussed and agreed. ISWG agreed that the Chairman and Secretariat should, after the meeting, produce a revised text of Part B for consideration by MSC 76. That revised text is attached as annex to this document.

3 The guidance includes text in [ ] relating to the control measures. This text has been developed by the Contact Group on Regulation 9. That Contact Group continues its work and the outcome of its considerations will be reported in due course.

Action requested of the Committee

3 The Committee is invited to note the above, consider the attached text and take action as appropriate.

***

ANNEX

PART B

RECOMMENDED GUIDANCE REGARDING THE PROVISIONS OF CHAPTER XI-2 OF THE ANNEX TO THE INTERNATIONAL CONVENTION FOR THE SAFETY OF LIFE AT SEA, 1974 AS AMENDED AND PART A OF THIS CODE

TABLE OF CONTENTS

5 DECLARATION OF SECURITY

6 OBLIGATIONS OF THE COMPANY

Relevant guidance is provided under sections 8, 9 and 13.

7 SHIP SECURITY

Relevant guidance is provided under sections 8, 9 and 13.

8 SHIP SECURITY ASSESSMENT

9 SHIP SECURITY PLAN

10 RECORDS

No additional guidance.

11 COMPANY SECURITY OFFICER

Relevant guidance is provided under sections 8, 9 and 13.

12 SHIP SECURITY OFFICER

Relevant guidance is provided under sections 8, 9 and 13.

13 TRAINING AND DRILLS

14 PORT FACILITY SECURITY

Relevant guidance is provided under sections 15, 16 and 18.

15 PORT FACILITY SECURITY ASSESSMENT

	Sections
General	15.1 – 15.4
Identification and Evaluation of Important Assets and Infrastructure it is Important to Protect	15.5 – 15.8
Identification of the Possible Threats to the Assets and Infrastructure and the Likelihood of their Occurrence in Order to Establish and Prioritise Security Measures	15.9 – 15.12
Identification, Selection, and Prioritisation of Countermeasures and Procedural Changes and their Level of Effectiveness to Reduce Vulnerabilities	15.13 – 15.14
Identification of Vulnerabilities	15.15 – 15.16

16 PORT FACILITY SECURITY PLAN

	Sections
General	16.1 –16.6
Organization and Performance of Port Facility Security Duties	16.7 – 16.8
Access to the Port Facility	16.9 – 16.19
Restricted Areas within the Port Facility	16.20 – 16.28
Handling of Cargo	16.29 – 16.36
Delivery of Ship's Stores	16.37 – 16.43
Handling Unaccompanied Baggage	16.44 – 16.47
Monitoring the Security of the Port Facility	16.48 – 16.53
Differing Security Levels	16.54
Activities not covered by the Code	16.55
Declarations of Security	16.56
Audit, Review and Amendment	16.57 – 16.60
Approval of Port Facility Security Plans	16.57

17 PORT FACILITY SECURITY OFFICER

Relevant guidance is provided under sections 15, 16 and 18.

18 TRAINING AND DRILLS

	Sections
Port Facility Security Officer	18.1
Port Facility Personnel having specific Security Duties	18.2
All other Port Facility Personnel	18.3
Drills	18.4

19 VERIFICATION AND CERTIFICATION OF SHIPS

No additional guidance.

APPENDIX TO PART B

Appendix 1 – Declaration of Security

1 Introduction

General

1.1 This introduction outlines the processes envisaged in implementing the chapter XI-2 and the provisions of Part A of this Code and identifies the main elements on which guidance is offered.
It also sets down essential considerations, which should be taken into account when considering the application of the guidance relating to ships and port facilities.

1.2 If the reader's interest relates to ships alone, it is strongly recommended that this Part of the Code is still read as a whole, particularly the sections relating to port facilities.
The same applies to those whose primary interest are port facilities; they should also read the sections relating to ships.

1.3 The guidance provided in the following sections relates primarily to protection of the ship when it is at a port facility.
There could, however, be situations when a ship may pose a threat to the port facility, e.g. because, once within the port facility, it could be used as a base from which to launch an attack. When considering the appropriate security measures to respond to ship-based threats, those completing the Port Facility Security Assessment or preparing the Port Facility Security Plan should consider making appropriate adoptions to the guidance offered in the following sections.

Responsibilities of Contracting Governments

1.4 Contracting Governments have, under the provisions of chapter XI-2 and Part A of this Code, responsibilities, which include:

- setting the applicable security level;
- approving the Ship Security Plan and relevant amendments to an approved plan;
- verifying compliance with the provisions of chapter XI-2 and Part A of this Code and issuing to ships the International Ship Security Certificate;
- ensuring completion and approval of the Port Facility Security Assessment;
- designating the port facilities which will be required to appoint a Port Facility Security Officer and prepare a Port Facility Security Plan;
- approving the Port Facility Security Plan and relevant amendments to an approved plan; and
- exercising control measures.

1.5 Contracting Governments can designate, or establish, Designated Authorities within Government to undertake their security duties under the Code.
Contracting Governments or Designated Authorities may also delegate the undertaking of certain duties to Recognised Security Organizations outside Government.
Contracting Governments or Designated Authorities cannot delegate to a Recognized Security Organization the duty of:

- setting of the applicable security level;
- approving a Port Facility Security Assessment;
- designating the port facilities which will be required to appoint a Port Facility Security Officer and prepare a Port Facility Security Plan;

- approving a Port Facility Security Plan and subsequent amendments to an approved plan;
- exercising control measures; and
- establishing the requirements for a Declaration of Security.

Setting the Security Level

1.6 The setting of the security level applying at any particular time is the responsibility of Contracting Governments and can apply to ships and port facilities.
The Part A of the Code defines three security levels for international use. These are:

- Security Level 1, normal; the level at which ships and port facilities normally operate;
- Security Level 2, heightened; the level applying for as long as there is a heightened risk of a security incident; and
- Security Level 3, exceptional, the level applying for the period of time when there is the probable or imminent risk of a security incident.

The Company and the Ship

1.7 Any Company operating ships to which this Code applies has to appoint a Company Security Officer for the company and a Ship Security Officer for each of its ships. The responsibilities of these officers are defined, as are their training requirements and drills, in Part A of this Code.

1.8 The Company Security Officer's responsibilities include the completion of a Ship Security Assessment and of a Ship Security Plan for each ship to which the Code applies.

1.9 The Ship Security Plan should indicate the operational and physical security measures the ship should take to ensure it always operates at security level 1.
The plan should also indicate the additional, or intensified, security measures the ship itself can take to move to security level 2.
Furthermore, the plan should indicate the possible preparatory actions the ship could take to allow prompt response to the instructions that may be issued to the ship by the authorities responding at security level 3 to a security incident or threat.

1.10 The Ship Security Plan has to be approved by, or on behalf of, the Administration. The Company and Ship Security Officer should monitor the continuing relevance and effectiveness of the plan, including the undertaking of independent internal audits. Any amendments to specified elements of an approved plan have to be resubmitted for approval.

1.11 The ship has to carry an International Ship Security Certificate indicating that it complies with the requirements of chapter XI-2 and Part A of this Code. The Code includes provisions relating to the verification and certification of the ship's compliance with the requirements on an initial, renewal and intermediate verification basis.

[1.12 The International Ship Security Certificate is subject to port State control inspections but such inspections should not normally extend to examination of the Ship Security Plan itself.
The ship may be subject to additional control measures if there is reason to believe that the security of the ship has, or the port facilities it has served have, been compromised.

The ship may be required to provide information prior to port entry and it is the responsibility of the company that up-to-date information relating to the ownership and control of the ship is available on board.]

The Port Facility

1.13 Each Contracting Government has to ensure completion of a Port Facility Security Assessment of its port facilities. The Contracting Government, a Designated Authority or a Recognized Security Organization can conduct this assessment. The completed Port Facility Security Assessment has to be approved by the Contracting Governments concerned. This approval cannot be delegated. Port Facility Security Assessments should be periodically reviewed.

1.14 The Port Facility Security Assessment is fundamentally a risk analysis of all aspects of a port facility's operation in order to determine which part(s) are more susceptible, and/or more likely, to be the subject of attack.
Risk is defined as a function of the threat of an attack coupled with the vulnerability of the target and the consequences of an attack.

The assessment must include the following components:

- the perceived threat to port installations and infrastructure must be determined;
- the potential vulnerabilities identified; and
- the consequences of incidents calculated.

On completion of the analysis, it will be possible to produce an overall assessment of the level of risk.
The Port Facility Security Assessment will help determine which port facilities are required to appoint a Port Facility Security Officer and prepare a Port Facility Security Plan.

1.15 The responsibilities of the Port Facility Security Officer are defined, as are the requirements for training and drills in Part A of this Code. The Port Facility Security Officer is responsible for the preparation of the Port Facility Security Plan.

1.16 The Port Facility Security Plan should indicate the operational and physical security measures the port facility should take to ensure that it always operates at security level 1. The plan should also indicate the additional, or intensified, security measures the port facility can take to move to security level 2.
Furthermore the plan should indicate the possible preparatory actions the port facility could take to allow prompt response to the instructions that may be issued by the authorities responding at security level 3 to a security incident or threat.

1.17 The Port Facility Security Plan has to be approved by the port facility's Contracting Government or by the Designated Authority.
The Port Facility Security Officer should implement its provisions and monitor the continuing effectiveness and relevance of the approved plan, including commissioning independent internal audits of the application of the plan.
The Contracting Government or the Designated Authority may test the effectiveness of the plan. The Port Facility Security Assessment covering the port facility should be regularly reviewed. All these activities may lead to amendment of the approved plan. Any amendments to specified elements of an approved plan will have to be submitted for approval.

[1.18 Ships using port facilities may be subject to the port State control inspections and additional control measures outlined below.
The relevant authorities may request the provision of information regarding the ship, its cargo, passengers and ship's personnel prior to the ship's entry into port.
There may be circumstances in which entry into port could be denied.]

Information and Communication

1.19 Chapter XI-2 and Part A of this Code require Contracting Governments to provide certain information to the International Maritime Organization and for information to be made available to allow effective communication between Contracting Governments and between Company/Ship Security Officers and the Port Facility Security Officers responsible for the port facility their ships visit.

2 DEFINITIONS

No additional guidance.

3 APPLICATION

General

3.1 The guidance given in this Part of the Code should be taken into account when implementing the requirements of chapter XI-2 and Part A of this Code.

3.2 However, it should be recognized that the extent to which the guidance on ships applies will depend on the type of ship, its cargoes and/or passengers, its trading pattern and the characteristics of the port facilities visited by the ship.

3.3 Similarly, in relation to the guidance on port facilities, the extent to which this guidance applies will depend on the types of cargoes and/or passengers and the trading patterns of visiting ships.

4 RESPONSIBILITY OF CONTRACTING GOVERNMENTS

Security of Assessments and Plans

4.1 Contracting Governments should ensure that appropriate measures are in place to avoid unauthorized disclosure of, or access to, security sensitive material relating to Ship Security Assessments, Ship Security Plans, Port Facility Security Assessments and Port Facility Security Plans, and to individual assessments or plans.

Designated Authorities

4.2 Contracting Governments may appoint a Designated Authority within Government to undertake any, or all, of the duties set out in chapter XI-2 or Part A of this Code.

Recognized Security Organizations

4.3 Contracting Governments or Designated Authorities may authorize a Recognized Security Organization (RSO) to undertake certain security related activities, including:

.1 approval of Ship Security Plans, or amendments thereto, on behalf of the Administration;
.2 verification and certification of compliance of ships with the requirements of chapter XI-2 and Part A of this Code on behalf of the Administration; and
.3 conducting Port Facility Security Assessments required by the Contracting Government or by the Designated Authority.

4.4 An RSO may also advise Companies or port facilities on security matters, including Ship Security Assessments, Ship Security Plans, Port Facility Security Assessments and Port Facility Security Plans.
If they have done so they should not be authorised to approve any plan they were involved with.

4.5 When authorizing an RSO, Contracting Governments should give consideration to the competency of such an organization. An RSO should be able to demonstrate:

.1 expertise in relevant aspects of security;
.2 appropriate knowledge of ship and port operations, including knowledge of ship design and construction if providing services in respect of ships and port design and construction if providing services in respect of port facilities;
.3 their capability to assess the likely security risks that could occur during ship and port facility operations including the ship/port interface and how to minimise such risks;
.4 their ability to maintain and improve the expertise of their personnel;
.5 their ability to monitor the continuing trustworthiness of their personnel;
.6 their knowledge of the requirements chapter XI-2 and Part A of this Code and relevant national and international legislation and security requirements; and
.7 their knowledge of current security threats and patterns;
.8 their knowledge on recognition and detection of weapons, dangerous substances and devices;
.9 their knowledge on recognition of characteristics and behavioural patterns of persons who are likely to threaten security;
.10 their knowledge on techniques used to circumvent security measures; and
.11 their knowledge of security and surveillance equipment and systems and their operational limitations.

4.6 A Recognized Organization, as defined in Regulation I/6 and fulfilling the requirements of Regulation XI-1/1, may be appointed as a RSO provided it has the appropriate security related expertise listed in section 4.5.

4.7 A Port, Port or Harbour Authority or Port Facility operator may be appointed as an RSO provided it has the appropriate security related expertise listed in section 4.5.

Setting the Security Level

4.8 In setting the security level Contracting Governments should take account of general and specific threat information. Contracting Governments should set the security level applying to ships or port facilities at one of three levels:

- Security level 1: normal, the level at which the ship or port facility normally operates;
- Security level 2: heightened, the level applying for as long as there is a heightened risk of a security incident; and
- Security level 3: exceptional, the level applying for the period of time when there is the probable or imminent risk of a security incident.

4.9 Setting security level 3 should be an exceptional measure applying only when there is credible information that a security incident is probable or imminent.
Security level 3 should only be employed for the duration of the identified security threat or actual security incident.
While the security levels may change from security level 1, through security level 2 to security level 3, it is also possible that the security levels will change directly from security level 1 to security level 3.

4.10 At all times the Master of a ship has the ultimate responsibility for the safety of the ship. Even at security level 3 a Master may seek clarification or amendment of instructions issued by those responding to a security incident, or threat thereof, if there are reasons to believe that compliance with any instruction may imperil the safety of the ship.

4.11 The Company Security Officer (CSO) or the Ship Security Officer (SSO) should liase at the earliest opportunity with the Port Facility Security Officer (PFSO) of the port facility the ship is intended to visit to establish the security level applying for that ship at the port facility. Having established contact with a ship, the PFSO should advise the ship of any subsequent change in the port facility's security level and should provide the ship with any relevant security information.

4.12 While there may be circumstances when an individual ship may be operating at a higher security level than the port facility it is visiting, there will be no circumstances when a ship can have a lower security level than the port facility it is visiting.
If a ship has a higher security level than the port facility it intends to use, the CSO or SSO should advise the PFSO without delay.
The PFSO should undertake an assessment of the particular situation in consultation with the CSO or SSO and agree on appropriate security measures with the ship.

4.13 Contracting Governments should consider how information on changes in security levels should be promulgated rapidly.
Administrations may wish to use NAVTEX messages or Notices to Mariners as the method for notifying such changes in security levels to ship and CSO and SSO. Or, they may wish to consider other methods of communication that provide equivalent or better speed and coverage. Contracting Governments should establish means of notifying PFSOs of changes in security levels.

Contracting Governments should compile and maintain the contact details for a list of those who need to be informed of changes in security levels.
Whereas the security level need not be regarded as being particularly sensitive, the underlying threat information may be highly sensitive. Contracting Governments should give careful consideration to the type and detail of the information conveyed and the method by which it is conveyed, to SSOs, CSOs and PFSOs.

Information on Port Facility Security Plans

4.14 Contracting Governments should consider carefully the promulgation of information relating to port facilities within their territory which, following a PFSA, have been determined as meeting the provisions of regulation XI-2/2.2.
Those port facilities that do **not** need to have a PFSP when the PFSA is first undertaken may need to receive, from time to time, ships requiring security protection and if the circumstances alter may need a PFSP, possibly at short notice in the future.
Similarly, port facilities that are designated as needing a PFSP may subsequently no longer need one. It is clearly not desirable for information on whether a port facility is deemed to need a PFSP to be easily available or discernable. It is also undesirable to have a large burden of updating and checking the validity of information on port facilities across the globe.
However, it is necessary for CSOs and SSOs to know in advance of arrival who should be contacted to liase on security issues.
The Contracting Government or the Designated Authority should:

.1 retain the information on which port facilities have a PFSP centrally.
Certain information also has to be provided to the International Maritime Organization. It is for the Contracting Government to decide with whom it shares security information relating to individual PFSPs; and

.2 establish a domestic system in which there is central, regional, or port specific points of contact that cover all ports or a mix of these options that **does not identify** which of the ports do not have a PFSP. These points of contact should be made available widely and should be provided to the International Maritime Organisation. Approaching ships that wish to engage in ship port facility activity need only contact the appropriate point to ensure that the destination port is alert to its security status and intended arrival. The central or regional or port specific points of contact may be a PFSO or the contact point may establish a link between CSO or SSO and the PFSO.

Ports without Port Facility Security Plans

4.15 In the case of a port that does **not** have a PFSP (and therefore does not have a PFSO) the central or regional point of contact should be able to identify a suitably qualified person ashore who can arrange for appropriate security measures to be in place, if needed, for the duration of the ship's visit.

Government Contact Point

4.16 Contracting Governments should provide the contact details of Government officers to whom an SSO, a CSO and a PFSO can report security concerns.
These Government officers should assess such reports before taking appropriate action. Such reported concerns may have a bearing on the security measures falling under the jurisdiction of another Contracting Government.
In that case, the Contracting Governments should consider contacting their counterpart in the other Contracting Government to discuss whether remedial action is appropriate.
For this purpose, the contact details of the Government officers should be communicated to the International Maritime Organization.

Identification Documents

4.17 Contracting Governments are encouraged to issue appropriate identification documents to Government officials entitled to board ships or enter port facilities when performing their official duties and to establish procedures whereby the authenticity of such documents might be verified.

Fixed and Floating Platforms

4.18 Contracting Governments should establish appropriate security measures to enhance the security of fixed and floating platforms and to ensure that any security provisions applying to such platforms allow interaction with ships covered by this Code.[1]

Ships to which this Code does not apply

4.19 Contracting Governments should establish appropriate security measures to enhance the security of ships to which this Code does not apply and to ensure that any security provisions applying to such ships allow interaction with ships covered by this Code.

Incidents at Sea

4.20 Administrations should provide guidance to ships flying their flag on the action to be taken in accordance with security levels 1 to 3, if:

.1 there is an upwards change in the security level applying to the ship while it is at sea, e.g. because of the geographical area in which it is operating or relating to the ship itself; and
.2 there is a security incident or threat thereof involving the ship while at sea.

4.21 Administrations should provide guidance on the measures considered appropriate in the event of an attack on a ship or the identified risk of such an attack. This guidance should include information on the appropriate point of contact within the Administration and on the circumstances in which the Administration considers assistance should be sought from nearby coastal States and their police, security or armed forces.

[1]Refer to Establishment of Appropriate Measures to Enhance the Security of Ships, Port Facilities, and Fixed and Floating Platforms Not Covered by SOLAS Chapter XI-2, adopted by the Conference on Maritime Security by resolution [X].

Alternative Measures and Equivalent Arrangements

4.22 Contracting Governments may conclude bilateral or multilateral agreements to establish alternative security measures. However, these alternative measures must be at least as effective in providing and maintaining security as those specified in chapter XI-2 and in Part A of this Code.
When concluding such agreements, Contracting Governments should consult Administrations and other Contracting Governments with an interest.

[Control Measures

General

4.23 This section provides guidance on :

.1 control of ships in port;
.2 ships intending to enter the port of another Contracting Government; and
.3 no more favourable treatment for non-party ships and ships below convention size.

Control of Ships in Port

4.24 "Port": Regulation XI-2/9 is intended to apply to ships in port including ships at anchorages in close proximity to the port and to ships in the approaches to the port.[2]

4.25 "Officers duly authorized": are those persons appointed by the Contracting Government who should have the knowledge, expertise and legal status needed to exercise the control measures and the steps set out in regulation XI-2/9. Such officers should be responsible exclusively to the Government that gave them the authority to act.

4.26 "Clear grounds that the ship is not in compliance[3]": means evidence or reliable information that the ship, its equipment, its personnel, or its circumstances do not correspond substantially with the requirements of chapter XI-2 or Part A of this Code, taking into account the guidance given in this Part. Such evidence may arise from the duly authorized officer's general impressions or observations gained while verifying the International Ship Security Certificate or such evidence may arise from other sources. Examples of clear grounds include:

---

[2] Regulation XI-2/1 includes a definition of "port" that many Contracting Governments find useful and which is consistent with the intent of Regulation XI-2/9. On the other hand, many other Contracting Governments find the definition unnecessary, preferring that Contracting Parties would interpret the word "port" as for Regulation I/19, again consistently with the intent of this regulation. Any decision to delete the definition will require careful review of the whole of chapter XI-2, and of Parts A and B of this Code to check that each reference to the word "port" is consistent with the intended application of the requirements and of the guidance. If a definition is retained it will need to be consistent with the definition of port in Article 11 of UNCLOS.

[3] This guidance is very similar to that developed for safety and environmental protection in "Procedures for Port State Control" adopted by Assembly Resolution A787(19). "Clear grounds" is an expression that is well established in international law including UNCLOS (see Part XII, Section 7 and Articles 94.6, 108, 110 and 111). Some Contracting Governments do not see the need for additional guidance on what constitutes "clear grounds" whereas others comment that security is so different from the subject of these UNCLOS references that separate guidance is needed to avoid confusion.

.1 evidence from a review of the International Ship Security Certificate that it is clearly invalid;
.2 evidence that serious deficiencies exist in the security and surveillance equipment and systems, plans, documentation or arrangements required by chapter XI-2 and Part A of this Code;
.3 receipt of a report or complaint which, in the professional judgement of the duly authorized officer, contains reliable information clearly indicating that the ship does not comply with the requirements of chapter XI-2 or Part A of this Code;
.4 evidence that the master or ship's personnel is not familiar with essential shipboard plans, operations and exercises related to the security of the ship or that such operations or exercises have not been carried out;
.5 evidence that key ship's personnel members are not able to establish proper communication with any other key ship's personnel member on board the ship;
.6 evidence that the ship has embarked persons, or loaded stores or cargo at a port or from another ship where either the port facility or the other ship is in violation of chapter XI-2 or part A of this Code, and the ship in question has not taken appropriate, special or additional security measures or has not maintained appropriate ship security procedures; and
.7 evidence that the ship has embarked persons, or loaded stores or cargo at a port or from another ship where either the port facility or the other ship is not required to comply with chapter XI-2 or Part A of this, and the Ship Security Plan does not contain procedures for ensuring the security of such transactions, or such procedures were not followed.

4.27 Officers duly authorized by a Contracting Government (officers duly authorised) may take measures, consistent with international law, to ensure the security of the port, ships, persons, stores and cargo in cases where the ship, although in compliance with chapter XI-2 and Part A of this Code, still gives rise to clear grounds for believing that the ship presents a security threat to the safety [or security] of persons, ships, port facilities or other property. Such situations include, but are not limited to where evidence exists that the ship has:

.1 received people, stores or cargo unloaded from an aircraft of unknown security status;
.2 rescued or recovered persons or goods as a result of rendering assistance at sea;
.3 reported that the cargo, stores or other materials on board may pose a security threat;
.4 reported that unauthorized persons are on board the ship or that unauthorized persons have had access the ship;
.5 issued a security alert that has not been followed by proper cancellation procedures; or
.6 otherwise engaged in activity that presents a threat to security.

4.28 Regulation XI-2/9.1.2 (and Regulation XI-2/9.2.4) uses the word "proportionate" to indicate that the officer duly authorized should ensure that any measures or steps imposed are reasonable in relation to the threat that the non-compliance poses to the safety [or security] of persons, ships, port facilities or other property.
Such measures or steps should, at the discretion of the officers duly authorized, be the minimum necessary to rectify or mitigate the non-compliance.
When non-compliance is suspected, the officers duly authorized should make every effort to ascertain whether there is a reason for the non-compliance that is unrelated to security.

4.29 Regulation XI-2/9.1.5 uses the phrase "corrected to the satisfaction of the Contracting Government" in connection with the lifting of any control measures or steps.
The phrase is considered to be the point in time when the officers duly authorized are of the opinion that the action taken to rectify the non-compliance has substantially eliminated the security threat.
The interpretation of this phrase is a matter of sovereign discretion exercised by the officers duly authorized and constrained by the compensation that would be payable to the ship for any loss or damage suffered due to it being unduly delayed or detained (Regulation XI-2/9.3.3.1 refers).

4.30 Where the non-compliance is either a defective item of equipment or system or faulty documentation which cannot be remedied in the port of inspection, the Contracting Government concerned may allow the ship to sail to another port provided that any conditions agreed between the Contracting Government, the Contracting Government of the next port of call and the Administration are met.
Such conditions should ensure that the ship is only released from further control measures when the non-compliance has been rectified to the satisfaction of the Contracting Government that first imposed the control measures.
Such conditions should also include confirmation from the Administration that remedial action has been taken.
If a ship does not comply with the control measures or conditions, the Contracting Government should immediately alert the next port(s) of call if known, the Administration and all other authorities it considers appropriate.

Ships intending to enter the port of another Contracting Government

4.31 Regulations XI-2/9.2.1.3 and XI-2/9.2.1.4 use the phrase "relevant ship/port interface". Given the definition "ship/port facility interface" provided in regulation XI-2/1.2[.2] guidance is only needed in respect of what is meant by the word "relevant".
An interface is "relevant" if it results in cargo, stores, [fuel, provisions,] passengers, ship's personnel or other persons being on board on arrival at the port from which the request for information is made. Or, in the case of ships entering a port in ballast, the relevant ship/port interface(s) are those where cargo and passengers were offloaded on [the] route to the port.

4.32 Regulation XI-2/9.2.1.5 introduces the term "relevant ship to ship activity" which is defined in Regulation XI-2/1.2[.2] and the footnote associated with that regulation.

4.33 Regulation XI-2/9.2.1.6 uses the phrase "other practical security related information" which is intended to assist with ensuring the safety [or security] of persons, port facilities, ships and other property.
Such information may also be used in the evaluation of whether the ship complies with the requirements of chapter XI-2 and Part A of this Code. Examples of such information include:

.1 name of the ship and previous name(s) if it has changed within the last 12 months;
.2 States of registry [(and or State whose flag the ship is entitled to fly)] and previous States of registry [(or flag)] if the ship has changed [(registry or)] flags within the last 12 months;
.3 IMO number or, if no IMO number has been assigned, the official number;
.4 name of the registered owner [(or the registered bareboat charterer, if any)] of the ship;
.5 name of the Company;

.6 name of the charterer of the ship;
.7 name of the classification society of the ship [, or of the recognised organisation or of the recognised security organisation involved in the survey, verification and certification of that ship];
.8 general description of cargo on board the ship;
.9 location of the ship at the time the report is made;
.10 crew list; and
.11 passenger list.

[Editorial Note: Regulation XI-2/9.2.3 dealing with the recording of the information associated with Regulation XI-2/9.2.1.3 to 6 needs to be drafted before any necessary guidance can be prepared.]

4.34 Regulation XI-2/9.3.2 requires the communication of all known facts to the authorities of relevant States when entry into a port is denied or the ship is expelled from the port.
This communication should consist of the following when known:

.1 name of ship, port of registry, IMO number, ship type and cargo;
.2 reason for denying entry or expulsion from port or port areas;
.3 the nature of any security non-compliance, if relevant;
.4 details of any attempts made to rectify any non-compliance, including any conditions imposed on the ship for the voyage, if relevant;
.5 declared port(s) of call;
.6 time of departure and likely estimated time of arrival at those ports;
.7 any instructions given to ship, e.g., reporting on route;
.8 the security level at which the ship is currently operating;
.9 copies of any communications the Contracting Government has had with the Administration;
.10 contact point within the Contracting Government making the report for the purpose of obtaining further information;
.11 crew list;
.12 passenger list, if relevant; and
.13 any other relevant information.

4.35 Relevant States to contact should include those along the ship's intended passage to its ext port, particularly if the ship intends to enter the territorial water of that coastal State
Others relevant States could include previous ports of call, so that further information might be obtained or potential security issues in the previous port can be resolved.

No more favourable treatment for non-party ships and ships below convention size[4].

[4] It is debatable whether this guidance is needed given that it is not referred to in Regulation XI-2/9. Some Contracting Governments prefer to include it, others would like to see substantial amendment, while others prefer its deletion. The subject of "no more favourable treatment" is addressed in Article I(3) of the 1988 SOLAS Protocol, and this subject is not mentioned in either the articles of, or the regulations annexed to, the Convention
For ships below convention size it has been suggested that, if anything needs to be stated about such ships, this should be the subject of a Conference Resolution.

4.36 Contracting Governments should encourage ships to which chapter XI-2 and Part A of this Code does not apply and ships flying the flag of States which are not parties to the Convention to comply with the requirements of chapter XI-2 and Part A of this Code.

4.37 Article II(3) of the 1978 SOLAS Protocol and Article I(3) of the 1988 SOLAS Protocol provide that no more favourable treatment is to be given to the ships of States which are not party to the Convention and the 1978 SOLAS Protocol or to the 1988 SOLAS Protocol.
All Contracting Government should, as a matter of principle, apply control procedures to ships of non-parties and to ships below convention size in order to ensure an equivalent level of security as provided by compliance with chapter XI-2 and Part A of this Code.

4.38 In applying the no more favourable treatment clause substantial compliance with the provisions and criteria specified must be required before the ship is allowed in port.
Should any doubt arise, in order to confirm that the ship does not correspond substantially with the requirements of chapter XI-2 or Part A of this Code, an inspection should be conducted.

4.39 As the above mentioned ships are not required to comply with the provisions of chapter XI-2 or Part A of this Code, officers duly authorized should, when informed of the intention of such a ship to enter one of their ports, ensure by inspection if necessary that an equivalent level of security exists.

4.40 If the ship has some form of certification other than the required certificate, the officer duly authorized may take the form and content of that document into account in the evaluation of the ship.
In all circumstances, the officer duly authorized should be satisfied that neither the ship nor the ship's personnel pose a security threat to the safety [or security] of persons, or of ships [or port facilities] or other property.

4.41 The conditions of, and on, such a ship and its security [measures and] arrangements and the certification of the ship's personnel and the flag State's minimum safe manning standards should be comparable with the aims of the provisions of the Convention [and the 1988 SOLAS Protocol]; otherwise the ship should be subject to such restrictions as are necessary to obtain a comparable level of security.

4.42 Duly authorized officers may take into account any security clearance issued by another Contracting Government within the last [*time period*].

4.43 Officers duly authorized should at all times use their professional judgment to determine whether a ship complies with the requirements applicable requirement.
In doing so the officer duly authorized should be guided by the principle that a departure from the requirements of chapter XI-2 or Part A of this Code, taking into account the guidance given in this Part, could constitute a security threat. **]**

5 DECLARATION OF SECURITY

General

5.1 A Declaration of Security (DoS) should be completed when the Contracting Government of the port facility deems it to be necessary.

5.1.1 The need for a DoS may be indicated by the results of the Port Facility Security Assessment (PFSA) and the reasons and circumstances in which a DoS is required should be set out in the Port Facility Security Plan (PFSP).

5.2 It is envisaged that it will be the Port Facility Security Officer (PFSO) who requests completion of a DoS. It is likely that a DoS will be requested at higher security levels, when a ship has a higher security level than the port facility, and for ship/port interface activities that pose a higher risk to people, property or the environment for reasons specific to that ship, including its cargo or passengers or the circumstances at the port facility or a combination of these factors.

5.3 A PFSO may also initiate a DoS prior to ship/port interfaces that are identified in the approved PFSA as being of particular concern. Examples may include the embarking or disembarking passengers, and the transfer, loading or unloading of dangerous cargoes.
The PFSA may also identify facilities at or near highly populated areas or economically significant operations that warrant a DoS.

5.4 The main purpose of a DoS is to detail the agreement reached between the ship and the port facility as to the respective security measures each will undertake in respect of a specific ship/port interface or a series of interfaces between the ship and the port facility.

5.4.1 The agreed DoS should be signed and dated by both the PFSO and the Ship Security Officer (SSO) to indicate compliance with chapter XI-2 and part A of this Code and should include its duration, the relevant security level, or levels, if the ship has a higher security level than the port facility, and the contact point.

5.4.2 A change in the security level may require that a new or revised DoS be completed.

5.5 The DoS should be completed in English, French or Spanish or in a language common to both the PFSO and SSO.

5.5.1 As completed DoS will contain security sensitive information appropriate measures should be taken to ensure that its confidentiality is protected.

5.6 The person responsible for security at a port which does not have a PFSO or PFSP may initiate a DoS when a ship to which chapter XI-2 and Part A of this Code applies intends to use such a port.

5.7 A model DoS is included in Appendix 1 to this Part.

6 OBLIGATIONS OF THE COMPANY

Relevant guidance is provided under sections 8, 9 and 13.

7 SHIP SECURITY

Relevant guidance is provided under sections, 8, 9 and 13.

8 SHIP SECURITY ASSESSMENT

Security Assessment

8.1 The Company Security Officer (CSO) is responsible for ensuring that a Ship Security Assessment (SSA) is carried out for each of the ships in the Company's fleet.
While the CSO need not necessarily personally undertake all the duties associated with the post, the ultimate responsibility for ensuring that they are properly performed remains with the individual CSO.

8.2 Prior to commencing the SSA, the CSO should ensure that advantage is taken of information available on the assessment of threat for the ports at which the ship will call or at which passengers embark or disembark and about the port facilities and their protective measures. The CSO should study previous reports on similar security needs.
Where feasible, the CSO should meet with appropriate persons on the ship and in the port facilities to discuss the purpose and methodology of the assessment.
The CSO should follow any specific guidance offered by the Contracting Governments.

8.3 The CSO should obtain and record the information required to conduct an assessment, including:

.1 the general layout of the ship;
.2 the location of areas which should have restricted access, such as navigation bridge, machinery spaces of category A and other control stations as defined in chapter II-2, etc.;
.3 the location and function of each actual or potential access point to the ship;
.4 the open deck arrangement including the height of the deck above the water and, when alongside at any port facilities regularly served, the relative height to the quay at various levels of the tide and at various stages of cargo working;
.5 the cargo spaces and stowage arrangements;
.6 the locations where the ship's stores and essential maintenance equipment is stored;
.7 the locations where unaccompanied baggage is stored;
.8 the emergency and stand-by equipment available to maintain essential services;
.9 numerical strength, reliability and security duties of the ship's personnel;
.10 existing security and safety equipment for the protection of passengers and ship's personnel;
.11 escape and evacuation routes and assembly stations which have to be maintained to ensure the orderly and safe emergency evacuation of the ship;
.12 existing agreements with private security companies providing ship/waterside security services; and
.13 existing security measures and procedures in effect, including inspection and, control procedures, pass systems, surveillance and monitoring equipment, personnel identification documents and communication, alarms, lighting, access control and other appropriate systems.

On-scene Security Survey

8.4 The on-scene security survey should examine and evaluate existing shipboard protective measures, procedures and operations for:

.1 ensuring the performance of all ship security duties;
.2 monitoring restricted areas to ensure that only authorized persons have access;
.3 controlling access to the ship, including pass systems;
.4 monitoring of deck areas and areas surrounding the ship;
.5 controlling the embarkation of persons and their effects (accompanied and unaccompanied baggage and ship's personnel personal effects);
.6 supervising the handling of cargo and the delivery of ship's stores; and
.7 ensuring that ship security communication, information, and equipment are readily available.

8.5 The SAA should examine each identified point of access, including open weather decks, and evaluate its potential for use by individuals who might seek to breach security. This includes individuals having legitimate access as well as those who seek to obtain unauthorized entry.

8.6 The SSA should consider the continuing relevance of the existing security measures and guidance, procedures and operations, under both routine and emergency conditions and should determine security guidance including:

.1 the restricted areas;
.2 the response procedures to fire or other emergency conditions;
.3 the level of supervision of the ship's personnel, passengers, visitors, vendors, repair technicians, dock workers, etc.;
.4 the frequency and effectiveness of security patrols;
.5 the access control systems, including pass systems;
.6 the security communications systems and procedures;
.7 the security doors, barriers and lighting; and
.8 the security and surveillance equipment and systems, if any.

8.7 The SSA should consider the persons, activities, services and operations that it is important to protect, including:

.1 the ship;
.2 passengers, visitors, vendors, repair technicians, port facility personnel, etc;
.3 the ship's personnel;
.4 the capacity to maintain safe navigation and emergency response;
.5 the cargo, particularly dangerous goods or hazardous substances;
.6 the ship's stores;
.7 the ship security communication equipment and systems, if any; and
.8 the ship's security surveillance equipment and systems, if any.

8.8 The SSA should consider all possible threats, which may include:

.1 damage to, or destruction of, the ship [or of a port facility], e.g. by bombing, arson, sabotage or vandalism;
.2 hijacking or seizure of the ship or of persons on board;
.3 tampering with cargo, essential ship equipment or systems or ship's stores;

.4 unauthorized access or use, including presence of stowaways;
.5 smuggling weapons or equipment, including weapons of mass destruction;
.6 use of the ship to carry perpetrators and their personal equipment; and
.7 use of the ship itself as a weapon or as a means to cause damage or destruction.

8.9 The SSA should take into account all possible vulnerabilities, which may include any:

.1 conflicts between safety and security measures;
.2 conflicts between shipboard duties and security assignments;
.3 watch-keeping duties, ship's personnel size, particularly with implications on crew fatigue, alertness and performance;
.4 training deficiencies; and
.5 insufficient, poorly maintained or poor quality or unsuitable security equipment and systems, including communication systems.

8.10 The CSO and SSO should always have regard to the effect that security measures may have on ship's personnel who will remain on the ship for long periods.
When developing security measures, particular consideration should be given to the convenience, comfort and personal privacy of the ship's personnel and their ability to maintain their effectiveness over long periods.

9 SHIP SECURITY PLAN

General

9.1 Preparation of the Ship Security Plan (SSP) is the responsibility of the Company Security Officer (CSO).
The content of each individual SSP should vary depending on the particular ship it covers.
The Ship Security Assessment (SSA) will have identified the particular features of the ship and the potential threats and vulnerabilities.
The preparation of the SSP will require these features to be addressed in detail.
Administrations may prepare advice on the preparation and content of a SSP.

9.2 All SSPs should:

.1 detail the organizational structure of security for the ship;
.2 detail the ship's relationships with the Company, port facilities, other ships and relevant authorities with security responsibility;
.3 detail the communication systems to allow effective continuous communication within the ship and between the ship and others, including port facilities;
.4 detail the basic security measures for security level 1, both operational and physical, that will always be in place;
.5 detail the additional security measures that will allow the ship to progress without delay to security level 2 and, when necessary, to security level 3; and
.6 provide for regular review, or independent audit, of the SSP and for its amendment in response to experience or changing circumstances.

9.3 Preparation of an effective SSP should rest on a thorough assessment of all issues that relate to the security of the ship, including, in particular, a thorough appreciation of the physical and operational characteristics, including the voyage pattern, of the individual ship.

9.4 All SSPs should be approved by, or on behalf of, the Administration. If an Administration uses a Recognised Security Organisation (RSO) to review or approve the SSP the RSO should not be associated with any other RSO that prepared, or assisted in the preparation of, the plan.

9.5 CSOs and Ship Security Officers (SSOs) should develop procedures to:

.1 assess the continuing effectiveness of the SSP; and
.2 prepare amendments of the plan subsequent to its approval.

9.6 The security measures included in the SSP should be in place when the initial verification for compliance with the requirements of chapter XI-2 and Part A of this Code will be carried out. Otherwise the process of issue to the ship of the required International Ship Security Certificate cannot be carried out.
If there is any subsequent failure of security equipment or systems, or suspension of a security measure for whatever reason, equivalent temporary security measures should be adopted, notified to, and agreed by, the Administration. The International Ship Security Certificate should be appropriately endorsed.

Organization and Performance of Ship Security Duties

9.7 In addition to the guidance given in section 9.2, the SSP should establish the following which relate to all security levels:

.1 the duties and responsibilities of all shipboard personnel with a security role;
.2 the procedures or safeguards necessary to allow such continuous communications to be maintained at all times;
.3 the procedures needed to assess the continuing effectiveness of security procedures and any security and surveillance equipment and systems, including procedures for identifying and responding to equipment or systems failure or malfunction;
.4 the procedures and practices to protect security sensitive information held in paper or electronic format;
.5 the type and maintenance requirements, of security and surveillance equipment and systems, if any;
.6 the procedures to ensure the timely submission, and assessment, of reports relating to possible breaches of security or security concerns; and
.7 procedures to establish, maintain and up-date an inventory of any dangerous goods or hazardous substances carried on board, including their location.

9.8 The remainder of this section addresses specifically the security measures that could be taken at each security level covering:

.1 Access to the Ship by ship's personnel, passengers, visitors, etc;
.2 Restricted Areas on the Ship;
.3 Handling of Cargo;
.4 Delivery of Ship's Stores;
.5 Handling Unaccompanied Baggage; and
.6 Monitoring the Security of the Ship.

Access to the Ship

9.9 The SSP should establish the security measures covering the following means of access to the ship:

.1 access ladders;
.2 access gangways;
.3 access ramps;
.4 access doors, side scuttles, windows and ports;
.5 mooring ropes and anchor chains;
.6 cranes and hoisting gear; and
.7 other access points identified in the SSA.

9.10 For each of these the SSP should identify the appropriate locations where access restrictions or prohibitions should be applied for each of the security levels. For each security level the SSP should establish the type of restriction or prohibition to be applied and the means of enforcing them.

9.11 The SSP should establish for each security level the means of identification required to allow access to the ship and for individuals to remain on the ship without challenge, this may involve developing an appropriate pass system allowing for permanent and temporary passes, for ship's personnel and visitors respectively.
Any ship pass system should, when it is practicable to do so, be co-ordinated with that applying to the port facility.
Passengers should be able to prove their identity by boarding passes, tickets, etc., but should not be permitted to access restricted areas unless supervised.
The SSP should establish provisions to ensure that the pass systems are regularly updated, and that abuse of procedures should be subject to disciplinary action.

9.12 Those unwilling or unable to establish their identity and/or to confirm the purpose of their visit when requested to do so should be denied access to the ship and their attempt to obtain access should be reported to the SSOs, the CSOs, the Port Facility Security Officer (PFSO) and national or local authorities with security responsibilities.

9.13 The SSP should establish the frequency of application of any access controls particularly if they are to be applied on a random, or occasional, basis.

Security Level 1

9.14 At security level 1, the SSP should establish the security measures to control access to the ship, where the following may be applied:

.1 checking the identity documents of all persons seeking to board the ship and confirming their reasons for doing so by checking joining instructions, passenger tickets, boarding passes, work orders etc;
.2 for those not employed on the ship, restricting access to exclude those unable to establish their identity;
.3 in liaison with the port facility the ship should ensure that designated secure areas are established in which inspections and searching of people, baggage (including carry on items), personal effects, vehicles and their contents can take place;

.4 in liaison with the port facility the ship should ensure that vehicles destined to be loaded on board car carriers, ro-ro and other passenger ships are subjected to search prior to loading, in accordance with the frequency required in the SSP;
.5 segregating checked persons and their personal effects from unchecked persons and their personal effects;
.6 segregating embarking from disembarking passengers;
.7 identification of access points that should be secured or attended to prevent unauthorized access;
.8 securing, by locking or other means, access to unattended spaces adjoining areas to which passengers and visitors have access; and
.9 providing security briefings to all ship personnel on possible threats, the procedures for reporting suspicious persons, objects or activities and the need for vigilance.

9.15 At security level 1, all those seeking to board a ship should be liable to search. The frequency of such searches, including random searches, should be specified in the approved SSP and should be specifically approved by the Administration. Such searches may best be undertaken by the port facility in close co-operation with the ship and in close proximity to it.

Security Level 2

9.16 At security level 2, the SSP should establish the security measures to be applied to protect against a heightened risk of a security incident to ensure higher vigilance and tighter control, which may include:

.1 assigning additional personnel to patrol deck areas during silent hours to deter unauthorised access;
.2 limiting the number of access points to the ship, identifying those to be closed and the means of adequately securing them;
.3 deterring access to the ship, including the provision of boat patrols on the waterside of the ship;
.4 establishing a restricted area on the shore-side of the ship, in close co-operation with the port facility;
.5 increasing the frequency and detail of searches of people, personal effects, and vehicles;
.6 escorting visitors on the ship; and
.7 providing additional specific security briefings to all ship personnel on any identified threats, re-emphasising the procedures for reporting suspicious persons, objects, or activities and the stressing the need for increased vigilance.

Security Level 3

9.17 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

.1 limiting access to a single, controlled, access point;
.2 granting access only to those responding to the security incident or threat thereof;
.3 directions of persons on board;
.4 suspension of embarkation or disembarkation;

.5 suspension of cargo handling operations, deliveries etc;
.6 evacuation of the ship; and
.7 ship movement.

Restricted Areas on the Ship

9.18 The SSP should identify the restricted areas to be established on the ship, specify their extent, times of application, the security measures to be taken to control access to them and those to be taken to control activities within them. The purpose of restricted areas are to:

.1 prevent unauthorised access;
.2 protect passengers, ship's personnel, and personnel from port facilities or other agencies authorised to be on board the ship;
.3 protect sensitive security areas within the ship; and
.4 protect cargo and ship's stores from tampering.

9.19 The SSP should ensure that all restricted areas have clearly established policies and practices to control access to them.

9.20 The SSP should provide that all restricted areas should be clearly marked indicating that access to the area is restricted and that unauthorised presence within the area constitutes a breach of security.

9.21 Restricted areas may include:

.1 navigation bridge, machinery spaces of category A and other control stations as defined in chapter II-2;
.2 spaces containing security and surveillance equipment and systems and their controls and lighting system controls;
.3 ventilation and air-conditioning systems and other similar spaces;
.4 spaces with access to potable water tanks, pumps, or manifolds;
.5 spaces containing dangerous goods or hazardous substances;
.6 spaces containing cargo pumps and their controls;
.7 cargo spaces and spaces containing ship’s stores;
.8 crew accommodation; and
.9 any other areas as determined by the CSO, through the SSA to which access must be restricted to maintain the security of the ship.

Security Level 1

9.22 At security level 1, the SSP should establish the security measures to be applied to restricted areas, which may include:

.1 locking or securing access points;
.2 using surveillance equipment to monitor the areas;
.3 using guards or patrols; and
.4 using automatic intrusion detection devices to alert the ship’s personnel of unauthorized access.

Security Level 2

9.23 At security level 2, the frequency and intensity of the monitoring of, and control of access to restricted areas should be increased to ensure that only authorized persons have access. The SSP should establish the additional security measures to be applied, which may include:

.1 establishing restricted areas adjacent to access points;
.2 continuously monitoring surveillance equipment; and
.3 dedicating additional personnel to guard and patrol restricted areas.

Security Level 3

9.24 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operations with those responding and the port facility, which may include:

.1 the setting up of additional restricted areas on the ship in proximity to the security incident, or the believed location of the security threat, to which access is denied; and
.2 the searching of restricted areas as part of a search of the ship.

Handling of Cargo

9.25 The security measures relating to cargo handling should:

.1 prevent tampering, and
.2 prevent cargo that is not meant for carriage from being accepted and stored on board the ship.

9.26 The security measures should include inventory control procedures at access points to the ship. Once on board the ship, cargo should be capable of being identified as having been approved for loading onto the ship. In addition, security measures should be developed to ensure that cargo, once on board, is not tampered with.

Security Level 1

9.27 At security level 1, the SSP should establish the security measures to be applied during cargo handling, which may include:

.1 routine checking of cargo, cargo transport units and cargo spaces prior to, and during, cargo handling operations;
.2 checks to ensure that cargo being loaded matches the cargo documentation;
.3 ensuring, in liaison with the port facility, that vehicles to be loaded on board car-carriers, ro-ro and passenger ships are subjected to search prior to loading, in accordance with the frequency required in the SSP; and
.4 checking of seals or other methods used to prevent tampering.

9.28 Checking of cargo may be accomplished by the following means:

.1 visual and physical examination; and
.2 using scanning/detection equipment, mechanical devices, or dogs.

9.29 When there are regular, or repeated, cargo movement the CSO or SSO may, in consultation with the port facility, agree arrangements with shippers or others responsible for such cargo covering off-site checking, sealing, scheduling, supporting documentation, etc. Such arrangements should be communicated to and agreed with the PFSO concern.

Security Level 2

9.30 At security level 2, the SSP should establish the additional security measures to be applied during cargo handling, which may include:

.1 detailed checking of cargo, cargo transport units and cargo spaces;
.2 intensified checks to ensure that only the intended cargo is loaded;
.3 intensified searching of vehicles to be loaded on car-carriers, ro-ro and passenger ships; and
.4 increased frequency and detail in checking of seals or other methods used to prevent tampering.

9.31 Detailed checking of cargo may be accomplished by the following means:

.1 increasing the frequency and detail of visual and physical examination;
.2 increasing the frequency of the use of scanning/detection equipment, mechanical devices, or dogs; and
.3 co-ordinating enhanced security measures with the shipper or other responsible party in addition to an established agreement and procedures.

Security Level 3

9.32 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

.1 suspension of the loading or unloading of cargo; and
.2 verify the inventory of dangerous goods and hazardous substances carried on board, if any, and their location.

<u>Delivery of Ship's Stores</u>

9.33 The security measures relating to the delivery of ship's stores should:

.1 ensure checking of ship's stores and package integrity;
.2 prevent ship's stores from being accepted without inspection;
.3 prevent tampering; and
.4 prevent ship's stores from being accepted unless ordered.

9.34 For ships regularly using the port facility it may be appropriate to establish procedures involving the ship, its suppliers and the port facility covering notification and timing of deliveries and their documentation. There should always be some way of confirming that stores presented for delivery are accompanied by evidence that they have been ordered by the ship.

Security Level 1

9.35 At security level 1, the SSP should establish the security measures to be applied to during delivery of ship's stores, which may include:

.1 checking to ensure stores match the order prior to being loaded on board; and
.2 ensuring immediate secure stowage of ship's stores.

Security Level 2

9.36 At security level 2, the SSP should establish the additional security measures to be applied during delivery of ship's stores by exercising checks prior to receiving stores on board and intensifying inspections.

Security Level 3

9.37 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

.1 subjecting ship's stores to more extensive checking;
.2 preparation for restriction or suspension of handling of ship's stores; and
.3 refusal to accept ship's stores on board the ship.

Handling Unaccompanied Baggage

9.38 The SSP should establish the security measures to be applied to ensure that unaccompanied baggage (i.e. any baggage, including personal effects, which is not with the passenger or ship's personnel member at the point of inspection or search) is identified and subjected to appropriate screening, including searching, before it is loaded on board the ship.
It is not envisaged that such baggage will be subjected to screening by both the ship and the port facility, and in cases where both are suitably equipped, the responsibility for screening should rest with the port facility.
Close co-operation with the port facility is essential and steps should be taken to ensure that unaccompanied baggage is handled securely after screening.

Security Level 1

9.39 At security level 1, the SSP should establish the security measures to be applied when handling unaccompanied baggage to ensure that all unaccompanied baggage is screened or searched up to and including 100 percent, which may include use of x-ray screening.

Security Level 2

9.40 At security level 2, the SSP should establish the additional security measures to be applied when handling unaccompanied which should include 100 percent x-ray screening of all unaccompanied baggage.

Security Level 3

9.41 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

.1 subjecting such baggage to more extensive screening, for example x-raying it from at least two different angles;
.2 preparation for restriction or suspension of handling of unaccompanied baggage; and
.3 refusal to accept unaccompanied baggage on board the ship.

Monitoring the Security of the Ship

9.42 The ship should have the capability to monitor the ship, the restricted areas on board and areas surrounding the ship. Such monitoring capabilities may include use of:

.1 lighting;
.2 watch-keepers, security guards and deck watches including patrols, and
.3 automatic intrusion detection devices and surveillance equipment.

9.43 When used, automatic intrusion detection devices should activate an audible and/or visual alarm at a location that is continuously attended or monitored.

9.44 The SSP should establish the procedures and equipment needed at each security level and the means of ensuring that monitoring equipment will be able to perform continually, including consideration of the possible effects of weather conditions or of power disruptions.

Security Level 1

9.45 At security level 1, the SSP should establish the security measures to be applied which may be a combination of lighting, watch keepers, security guards or use of security and surveillance equipment to allow ship's security personnel to observe the ship in general, and barriers and restricted areas in particular.

9.46 The ship's deck and access points to the ship should be illuminated at all times while conducting ship/port interface activities or at a port facility or anchorage.
While underway, ships should use the maximum lighting available consistent with safe navigation, having regard to the provisions of the 1972 COLREGS.
The following should be considered when establishing the appropriate level and location of lighting:

.1 the ship's personnel should be able to detect activities beyond the ship, on both the shore side and the waterside;

.2 coverage should include the area on and around the ship;
.3 coverage should facilitate personnel identification at access points; and
.4 coverage may be provided through coordination with the port facility.

Security Level 2

9.47 At security level 2, the SSP should establish the additional security measures to be applied to enhance the monitoring and surveillance capabilities, which may include:

.1 increasing the frequency and detail of security patrols;
.2 increasing the coverage and intensity of lighting or the use of security and surveillance and equipment;
.3 assigning additional personnel as security lookouts; and
.4 ensuring coordination with waterside boat patrols, and foot or vehicle patrols on the shore-side, when provided.

9.48 Additional lighting may be necessary to protect against a heightened risk of a security incidents. When necessary, the additional lighting requirements may be accomplished by coordinating with the port facility to provide additional shore side lighting.

Security Level 3

9.49 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

.1 switching on of all lighting on, or illuminating the vicinity of, the ship;
.2 switching on of all on board surveillance equipment capable of recording activities on, or in the vicinity of, the ship;
.3 maximising the length of time such surveillance equipment can continue to record;
.4 preparation for underwater inspection of the hull of the ship; and
.5 initiation of measures, including the slow revolution of the ship's propellers, if practicable, to deter underwater access to the hull of the ship.

Differing Security Levels

9.50 The SSP should establish details of the procedures and security measures the ship could adopt if the ship is at a higher security level than that applying to a port facility.

Activities not covered by the Code

9.51 The SSP should establish details of the procedures and security measures the ship should apply when:

.1 it is at a port of a State which not a Contracting Government;
.2 it is interfacing with a ship to which this Code does not apply; and
.3 it is interfacing with fixed or floating platforms.

Declarations of Security

9.52 The SSP should detail how requests for DoS from a port facility will be handled.

Audit and Review

9.53 The SSP should establish how the CSO and the SSO intend to audit the continued effectiveness of the SSP and the procedure to be followed to review, update or amend the SSP. The independence of any internal audit should be ensured.

10 RECORDS

No additional guidance.

11 COMPANY SECURITY OFFICER

Relevant guidance is provided under sections 8, 9 and 13.

12 SHIP SECURITY OFFICER

Relevant guidance is provided under sections 8, 9 and 13.

13 TRAINING AND DRILLS

13.1 The Company Security Officer (CSO) and appropriate shore based Company personnel**,** and the Ship Security Officer (SSO), should have knowledge of, and receive training, in some or all of the following, as appropriate:

.1 security administration;
.2 relevant international conventions, codes and recommendations;
.3 relevant Government legislation and regulations;
.4 responsibilities and functions of other security organisations;
.5 methodology of ship security assessment;
.6 methods of ship security surveys and inspections;
.7 ship and port operations and conditions;
.8 ship and port facility security measures;
.9 emergency preparedness and response and contingency planning;
.10 instruction techniques for security training and education, including security measures and procedures;
.11 handling sensitive security related information and security related communications;
.12 knowledge of current security threats and patterns;
.13 recognition and detection of weapons, dangerous substances and devices;
.14 recognition of characteristics and behavioural patterns of persons who are likely to threaten security;
.15 techniques used to circumvent security measures;
.16 security equipment and systems and their operational limitations;

.17 methods of conducting audits, inspection, control and monitoring;
.18 methods of physical searches and non-intrusive inspections;
.19 security drills and exercises, including drills and exercises with port facilities; and
.20 assessment of security drills and exercises.

13.2 In addition the SSO should have adequate knowledge of, and receive training, in some or all of the following, as appropriate:

.1 the layout of the ship;
.2 the ship security plan and related procedures (including scenario-based training on how to respond);
.3 crowd management and control techniques;
.4 operations of security equipment and systems; and
.5 testing, calibration and whilst at sea maintenance of security equipment and systems.

13.3 Shipboard personnel having specific security duties should have sufficient knowledge and ability to perform their assigned duties, including:

.1 knowledge of current security threats and patterns;
.2 recognition and detection of weapons, dangerous substances and devices;
.3 recognition of characteristics and behavioural patterns of persons who are likely to threaten security;
.4 techniques used to circumvent security measures;
.5 crowd management and control techniques;
.6 security related communications;
.7 knowledge of the emergency procedures and contingency plans;
.8 operations of security equipment and systems;
.9 testing, calibration and whilst at sea maintenance of security equipment and systems,
.10 inspection, control, and monitoring techniques; and
.11 methods of physical searches of persons, personal effects, baggage, cargo, and ship's stores.

13.4 All other shipboard personnel should have sufficient knowledge and ability to perform their assigned duties, including:

.1 the meaning and the consequential requirements of the different security levels;
.2 knowledge of the emergency procedures and contingency plans;
.3 recognition and detection of weapons, dangerous substances and devices;
.4 recognition of characteristics and behavioural patterns of persons who are likely to threaten security; and
.5 techniques used to circumvent security measures.

13.5 The objective of drills and exercises is to ensure that shipboard personnel are proficient in all assigned security duties at all security levels and the identification of any security related deficiencies, which need to be addressed.

13.6 Detailed security drills intended to exercise the entire SSP should be conducted at least once a month, unless the special circumstances of the ship type and ports to be visited suggest otherwise, i.e. at shorter or longer intervals, and if there are significant changes to the SSP or the composition of the ship's personnel.

14 PORT FACILITY SECURITY

Relevant guidance is provided under section 15, 16 and 18.

15 PORT FACILITY SECURITY ASSESSMENT

General

15.1 The Port Facility Security Assessment (PFSA) may be conducted for a Contracting Government by:

.1 a Designated Authority within Government; and
.2 a Recognized Security Organization (RSO).

However, approval of a completed PFSA should only be given by the relevant Contracting Government or by the Designated Authority.

15.2 If a Contracting Government uses a RSO, to review or verify compliance of the PFSA, the RSO should not be associated with any other RSO that prepared or assisted in the preparation of that assessment.

15.3 A PFSA should address the following elements within a port facility:

.1 physical security;
.2 structural integrity;
.3 personnel protection systems;
.4 procedural policies;
.5 radio and telecommunication systems, including computer systems and networks;
.6 relevant transportation infrastructure;
.7 utilities; and
.8 other areas that may, if damaged or used for illicit observation, pose a risk to people, property, or operations within the port facility.

15.4 Those involved in a PFSA should be able to draw upon expert assistance in relation to:

.1 knowledge of current security threats and patterns;
.2 recognition and detection of weapons, dangerous substances and devices;
.3 recognition of characteristics and behavioural patterns of persons who are likely to threaten security;
.4 techniques used to circumvent security measures;
.5 methods used to cause a security incident;
.6 effects of explosives on structures and port facility service suppliers;
.7 port facility security;
.8 port business practices;

.9 contingency planning, emergency preparedness and response;
.10 physical security;
.11 radio and telecommunications systems, including computer systems and networks;
.12 transport and civil engineering; and
.13 ship and port operations.

Identification and evaluation of important assets and infrastructure it is important to protect

15.5 The identification and evaluation of important assets and infrastructure is a process through which the relative importance of structures and installations to the functioning of the port facility can be established.
This identification and evaluation process is important because it provides a basis for focusing mitigation strategies on those assets and structures which it is more important to protect from a security incident.
This process should take into account potential loss of life, the economic significance of the port, symbolic value, and the presence of Government installations.

15.6 Identification and evaluation of assets and infrastructure should be used to prioritise their relative importance for protection.
The primary concern should be avoidance of death or injury. It is also important to consider whether the port facility, structure or installation can continue to function without the asset, and the extent to which rapid reinstatement of normal functioning is possible.

15.7 Assets and infrastructure that may be important to protect include:

.1 accesses, entrances, approaches, and anchorages, manoeuvring and berthing areas;
.2 cargo facilities, terminals, storage areas, and cargo handling equipment;
.3 systems such as electrical distribution systems, radio and telecommunication systems and computer systems and networks;
.4 port vessel traffic management systems and aids to navigation;
.5 power plants, cargo transfer piping, and water supplies;
.6 bridges, railways, roads;
.7 port service vessels, including pilot boats, tugs, lighters etc;
.8 security and surveillance equipment and systems; and
.9 the waters adjacent to the port facility.

15.8 The clear identification of assets and infrastructure is essential to the evaluation of the port facility's security requirements, the prioritisation of protective measures, and decisions concerning the allocation of resources to better protect the port facility.
The process may involve consultation with the relevant authorities relating to structures adjacent to the port facility which could cause damage within the facility or be used for the purpose of causing damage to the facility or for illicit observation of the facility or for diverting attention.

Identification of the possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritise security measures

15.9 Possible acts that could threaten the security of assets and infrastructure, and the methods of carrying out those acts, should be identified to evaluate the vulnerability of a given asset or location to a security incident, and to establish and prioritise security requirements to enable planning and resource allocations.

Identification and evaluation of each potential act and its method should be based on various factors, including threat assessments by Government agencies.
By identifying and assessing threats those conducting the assessment do not have to rely on worst-case scenarios to guide planning and resource allocations.

15.10 The PFSA should include an assessment undertaken in consultation with the relevant national security organizations to determine:

.1 any particular aspects of the port facility, including the vessel traffic using the facility, which make it likely to be the target of an attack;
.2 the likely consequences in terms of loss of life, damage to property, economic disruption, including disruption to transport systems, of an attack on, or at, the port facility;
.3 the capability and intent of those likely to mount such an attack; and
.4 the possible type, or types, of attack.

producing an overall assessment of the level of risk against which security measures have to be developed.

15.11 The security incidents affecting assets and infrastructure may include:

.1 damage to, or destruction of, the port facility or of the ship, e.g. by bombing, arson, sabotage or vandalism;
.2 hijacking or seizure of the ship or of persons on board;
.3 tampering with cargo, essential ship equipment or systems or ship's stores;
.4 unauthorised access or use including presence of stowaways;
.5 smuggling weapons or equipment, including weapons of mass destruction;
.6 use of the ship to carry perpetrators and their personal equipment; and
.7 use of the ship itself as a weapon or as a means to cause damage or destruction.
.6 blockage; of port entrances, locks, approaches etc; and
.7 nuclear, biological and chemical attack.

15.12 The process may involve consultation with the relevant authorities relating to structures adjacent to the port facility which could cause damage within the facility or be used for the purpose of causing damage to the facility or for illicit observation of the facility or for diverting attention.

<u>Identification, selection, and prioritisation of countermeasures and procedural changes and their level of effectiveness in reducing vulnerability</u>

15.13 The identification and prioritisation of countermeasures is designed to ensure that the most effective security measures are employed to reduce the vulnerability of a port facility or ship/port interface to the possible threats.

15.14 Security measures should be selected on the basis of factors such as whether they reduce the probability of an attack and should be evaluated using information that includes:

.1 security surveys, inspections and audits;
.2 consultation with port facility owners and operators, and owners/operators of adjacent structures if appropriate;

.3 historical information on security incidents; and
.4 operations within the port facility.

Identification of vulnerabilities

15.15 Identification of vulnerabilities in physical structures, personnel protection systems, processes, or other areas that may lead to a security incident can be used to establish options to eliminate or mitigate those vulnerabilities. For example, an analysis might reveal vulnerabilities in a port facility's security systems or unprotected infrastructure such as water supplies, bridges etc that could be resolved through physical measures, e.g. permanent barriers, alarms, surveillance equipment etc.

15.16 Identification of vulnerabilities should include consideration of:

.1 waterside and shore-side access to the port facility and ships berthing at the facility;
.2 structural integrity of the piers, facilities, and associated structures;
.3 existing security measures and procedures, including pass systems;
.4 existing security measures and procedures relating to port services and utilities;
.5 measures to protect radio and telecommunication equipment, port services and utilities, including computer systems and networks;
.6 adjacent areas that may be exploited during, or for, an attack;
.7 existing agreements with private security companies providing waterside/shore-side security services;
.8 any conflicting policies between safety and security measures and procedures;
.9 any conflicting port facility and security duty assignments;
.10 any enforcement and personnel constraints;
.11 any deficiencies identified during training and drills; and
.12 any deficiencies identified during daily operation, following incidents or alerts, the report of security concerns, the exercise of control measures, audits etc.

16 PORT FACILITY SECURITY PLAN

General

16.1 Preparation of the Port Facility Security Plan (PFSP) is the responsibility of the Port Facility Security Officer (PFSO).
While the PFSO need not necessarily personally undertake all the duties associated with the post the ultimate responsibility for ensuring that they are properly performed remains with the individual PFSO.

16.2 The content of each individual PFSP should vary depending on the particular circumstances of the port facility, or facilities, it covers.
The PFSA will have identified the particular features of the port facility, and of the potential risks, that have led to the need to appoint a PFSO and to prepare a PFSP.
The preparation of the PFSP will require these features, and other local or national security considerations, to be addressed in the PFSP and for appropriate security measures to be established so as to minimise the likelihood of a breach of security and the consequences of potential risks.

Contracting Governments may prepare advice on the preparation and content of a PFSP.

16.3 All PFSPs should:

.1 detail the security organisation of the port facility,
.2 the organisation's links with other relevant authorities and the necessary communication systems to allow the effective continuous operation of the organisation and its links with others, including ships in port;
.3 detail the basic security level 1 measures, both operational and physical, that will be in place;
.4 detail the additional security measures that will allow the port facility to progress without delay to security level 2 and, when necessary, to security level 3, and
.5 provide for regular review, or independent audit, of the PFSP and for its amendments in response to experience or changing circumstances.

16.4 Preparation of an effective PFSP will rest on a thorough assessment of all issues that relate to the security of the port facility, including, in particular, a thorough appreciation of the physical and operational characteristics of the individual port facility.

16.5 Contracting Government should approve the PFSPs of the port facilities under their jurisdiction.
Contracting Governments should develop procedures to assess the continuing effectiveness of each PFSP and may require amendment of the PFSP prior to its initial approval or subsequent to its approval.
The PFSP should make provision for the retention of records of security incidents and threats, reviews, audits, training, drills and exercises as evidence of compliance with those requirements.

16.6 The security measures included in the PFSP should be in place within a reasonable period of the PFSP's approval and the PFSP should establish when each measure will be in place.
If there is likely to be any delay in their provision this should be discussed with the Contracting Government responsible for approval of the PFSP and satisfactory alternative temporary security measures that provide an equivalent level of security should be agreed to cover any interim period.

Organization and Performance of Port Facility Security Duties

16.7 In addition to the guidance given under section 16.3, the PFSP should establish the following which relate to all security levels:

.1 the role and structure of the port facility security organisation;
.2 the duties, responsibilities and training requirements of all port facility personnel with a security role and the performance measures needed to allow their individual effectiveness to be assessed;
.3 the port facility security organisation's links with other national or local authorities with security responsibilities;
.4 the communication systems provided to allow effective and continuous communication between port facility security personnel, ships in port and, when appropriate, with national or local authorities with security responsibilities;
.5 the procedures or safeguards necessary to allow such continuous communications to be maintained at all times;

.6 the procedures and practices to protect security sensitive information held in paper or electronic format;
.7 the procedures to assess the continuing effectiveness of security measures, procedures and equipment, including identification of, and response to, equipment failure or malfunction;
.8 the procedures to allow the submission, and assessment, of reports relating to possible breaches of security or security concerns;
.9 procedures relating to cargo handling;
.10 procedures covering the delivery of ship's stores;
.11 the procedures to maintain, and update, records of dangerous goods and hazardous substances and their location within the port facility; and
.12 the means of alerting and obtaining the services of waterside patrols and specialist search teams, including bomb searches and underwater searches.

16.8 The remainder of this section addresses specifically the security measures that could be taken at each security level covering:

.1 Access to the Port Facility;
.2 Restricted Areas within the Port Facility;
.3 Handling of Cargo;
.4 Delivery of Ship's Stores;
.5 Handling Unaccompanied Baggage; and
.6 Monitoring the Security of the Port Facility.

Access to the Port Facility

16.9 The PFSP should establish the security measures covering the means of access to the port facility.

16.10 For each of these the PFSP should identify the appropriate locations where access restrictions or prohibitions should be applied for each of the security levels. For each security level the PFSP should specify the type of restriction or prohibition to be applied and the means of enforcing them.

16.11 The PFSP should establish for each security level the means of identification required to allow access to the port facility and for individuals to remain within the port facility without challenge, this may involve developing an appropriate pass system allowing for permanent and temporary passes, for port facility personnel and all for visitors respectively.
Any port facility pass system should, when it is practicable to do so, be co-ordinated with that applying to ships that regularly use the port facility.
Passengers should be able to prove their identity by boarding passes, tickets, etc., but should not be permitted to access restricted areas unless supervised.
The PFSP should establish provisions to ensure that the pass systems are regularly updated, and that abuse of procedures should be subject to disciplinary action.

16.12 Those unwilling or unable to establish their identity and/or to confirm the purpose of their visit when requested to do so should be denied access to the port facility and their attempt to obtain access should be reported to the PFSO and national or local authorities with security responsibilities.

16.13 The PFSP should identify the locations where people, personal effects, and vehicle searches are to be undertaken. Such locations should be covered to facilitate continuous operation regardless of prevailing weather conditions, in accordance with the frequency laid down in the PFSP. Once subjected to search people, personal effects and vehicles should proceed directly to the restricted holding, embarkation or car loading areas.

16.14 The PFSP should establish separate locations for checked and unchecked persons and their effects and if possible separate areas for embarking/disembarking passengers, ship's personnel and their effects to ensure that unchecked persons are not able to come in contact with checked persons.

16.15 The PFSP should establish the frequency of application of any access controls particularly if they are to be applied on a random, or occasional, basis.

Security Level 1

16.16 At security level 1, the PFSP should establish the control points where the following security measures may be applied:

.1 establish the restricted areas which should be bound by fencing or other barriers to a standard which should be approved by the Contracting Government;
.2 checking identity documents and/or passes of all those seeking entry to the port facility in connection with a ship, including passengers, ship's personnel and visitors, confirming their reasons for doing so by checking joining instructions, passenger tickets, boarding passes, work orders, etc;
.3 checking vehicles used by those seeking entry to the port facility in connection with a ship;
.4 verification of the identity of port facility personnel and those employed within the port facility and their vehicles;
.5 for those not employed by, or within, the port facility restricting access to exclude those unable to establish their identity;
.6 undertaking searches of people, personal effects, vehicles and their contents; and
.7 identification of any access points not in regular use which should be permanently closed and locked.

16.17 At security level 1, all those seeking access to the port facility should be liable to search. The frequency of such searches, including random searches, should be specified in the approved PFSP and should be specifically approved by the Contracting Government.

Security Level 2

16.18 At security level 2, the PFSP should establish the additional security measures to be applied, which may include:

.1 assign additional personnel to guard access points and patrol perimeter barriers;
.2 limit the number of access points to the port facility, and identify those to be closed and the means of adequately securing them;
.3 provide for means of impeding movement through the remaining access points, e.g. security barriers;
.4 increase the frequency of searches of persons, personal effects, and vehicle;

.5 deny access to visitors who are unable to provide a verifiable justification for seeking access to the port facility; and
.6 use of patrol vessels to enhance waterside security;

Security Level 3

16.19 At security level 3, the port facility should ensure compliance with instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility, in close co-operation with those responding and the ships at the port facility, which may include:

.1 suspension of access to all, or part of, the port facility;
.2 granting access only to those responding to the security incident or threat thereof;
.3 suspension of pedestrian or vehicular movement within all, or part, of the port facility;
.4 increased security patrols within the port facility, if appropriate;
.5 suspension of port operations within all, or part, of the port facility;
.6 direction of vessel movements relating to all, or part, of the port facility; and
.7 evacuation of all, or part of, the port facility.

Restricted Areas within the Port Facility

16.20 The PFSP should identify the restricted areas to be established within the port facility, specify their extent, times of application, the security measures to be taken to control access to them and those to be taken to control activities within them.
The purpose of restricted areas is to:

.1 protect passengers, ship's personnel, port facility personnel and visitors, including those visiting in connection with a ship;
.2 protect the port facility;
.3 protect ships using, and serving, the port facility;
.4 protect sensitive security locations and areas within the port facility,
.5 to protect security and surveillance equipment and systems; and
.6 protect cargo and ship's stores from tampering.

16.21 The PFSP should ensure that all restricted areas have clearly established security measures to control:

.1 access by individuals;
.2 the entry, parking, loading and unloading of vehicles;
.3 movement and storage of cargo and ship's stores, and
.4 unattended luggage or personal effects.

16.22 The PFSP should provide that all restricted areas should be clearly marked indicating that access to the area is restricted and that unauthorised presence within the area constitutes a breach of security.

16.23 When automatic intrusion detection devices are installed they should alert a control centre which can respond to the triggering of an alarm.

16.24 Restricted areas may include:

.1 shore and waterside areas immediately adjacent to the ship;
.2 embarkation and disembarkation areas, passenger and ship's personnel holding and processing areas including search points;
.3 areas where loading, unloading or storage of cargo and stores is undertaken;
.4 locations where security sensitive information, including cargo documentation, is held;
.5 areas where dangerous goods and hazardous substances are held;
.6 vessel traffic management system control rooms, aids to navigation and port control buildings, including security and surveillance control rooms;
.7 areas where security and surveillance equipment are stored or located;
.8 essential electrical, radio and telecommunication, water and other utility installations; and
.9 other locations in the port facility where access by vessels, vehicles and individuals should be restricted.

16.25 The security measures may extend, with the agreement of the relevant authorities, to restrictions on unauthorised access to structures from which the port facility can be observed.

Security Level 1

16.26 At security level 1, the PFSP should establish the security measures to be applied to restricted areas, which may include:

.1 provision of permanent or temporary barriers to surround the restricted area whose standard should be accepted by the Contracting Government;
.2 provision of access points where access can be controlled by security guards when in operation and which can be effectively locked or barred when not in use;
.3 providing passes which must be displayed to identify individuals entitlement to be within the restricted area;
.4 clearly marking vehicles allowed access to restricted areas;
.5 providing guards and patrols;
.6 providing automatic intrusion detection devices, or surveillance equipment or systems to detect unauthorised access into, or movement within restricted areas; and
.7 control of the movement of vessels in the vicinity of ships using the port facility.

Security Level 2

16.27 At security level 2, the PFSP should establish the enhancement of the frequency and intensity of the monitoring of, and control of access to, restricted areas. The PFSP should establish the additional security measures, which may include:

.1 enhancing the effectiveness of the barriers or fencing surrounding restricted areas, including the use of patrols or automatic intrusion detection devices;
.2 reducing the number of access points to restricted areas and enhancing the controls applied at the remaining accesses;
.3 restrictions on parking adjacent to berthed ships;
.4 further restricting access to the restricted areas and movements and storage within them;

.5 use of continuously monitored and recording surveillance equipment;
.6 enhancing the number and frequency of patrols undertaken on the boundaries of the restricted areas and within the areas;
.7 establishing and restricting access to areas adjacent to the restricted areas; and
.8 enforcing restrictions on access by unauthorised craft to the waters adjacent to ships using the port facility.

Security Level 3

16.28 At security level 3, the port facility should ensure compliance with the instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility, in close co-operation with those responding and the ships at the port facility, which may include:

.1 the setting up of additional restricted areas within the port facility in proximity to the security incident, or the believed location of the security threat, to which access is denied; and
.2 preparing for the searching of restricted areas as part of a search of all, or part, of the port facility.

Handling of Cargo

16.29 The security measures relating to cargo handling should:

.1 prevent tampering, and
.2 prevent cargo that is not meant for carriage from being accepted and stored within the port facility.

16.30 The security measures should include inventory control procedures at access points to the port facility. Once within the port facility cargo should be capable of being identified as having been checked and accepted for loading onto a ship or for temporary storage in a restricted area while awaiting loading. It may be appropriate to restrict the entry of cargo to the port facility that does not have a confirmed date for loading.

Security Level 1

16.31 At security level 1, the PFSP should establish the security measures to be applied during cargo handling, which may include:

.1 routine checking of cargo, cargo transport units and cargo storage areas within the port facility prior to, and during, cargo handling operations;
.2 checks to ensure that cargo entering the port facility matches the delivery note or equivalent cargo documentation;
.3 searches of vehicles; and
.4 checking of seals and other methods used to prevent tampering upon entering the port facility and upon storage within the port facility.

16.32 Checking of cargo may be accomplished by some or all of the following means:

.1 visual and physical examination; and
.2 using scanning/detection equipment, mechanical devices, or dogs.

16.33 When there are regular, or repeated, cargo movement the Company Security Officer (CSO) or the Ship Security Officer (SSO) may, in consultation with the port facility, agree arrangements with shippers or others responsible for such cargo covering off-site checking, sealing, scheduling, supporting documentation, etc. Such arrangements should be communicated to and agreed with the PFSO concern.

Security Level 2

16.34 At security level 2, the PFSP should establish the additional security measures to be applied during cargo handling to enhance control, which may include:

.1 detailed checking of cargo, cargo transport units and cargo storage areas within the port facility;
.2 intensified checks, as appropriate, to ensure that only the documented cargo enters the port facility, is temporarily stored there and then loaded onto the ship;
.3 intensified searches of vehicles; and
.4 increased frequency and detail in checking of seals and other methods used to prevent tampering.

16.35 Detailed checking of cargo may be accomplished by some or all of the following means:

.1 increasing the frequency and detail of checking of cargo, cargo transport units and cargo storage areas within the port facility (visual and physical examination);
.2 increasing the frequency of the use of scanning/detection equipment, mechanical devices, or dogs; and
.3 co-ordinating enhanced security measures with the shipper or other responsible party in addition to an established agreement and procedures.

Security Level 3

16.36 At security level 3, the port facility should ensure compliance with the instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility, in close co-operation with those responding and the ships at the port facility, which may include:

.1 restriction or suspension of cargo movements or operations within all, or part, of the port facility or specific ships; and
.2 verifying the inventory of dangerous goods and hazardous substances held within the port facility and their location.

<u>Delivery of Ship's Stores</u>

16.37 The security measures relating to the delivery of ship's stores should:

.1 ensure checking of ship's stores and package integrity;
.2 prevent ship's stores from being accepted without inspection;
.3 prevent tampering;
.4 prevent ship's stores from being accepted unless ordered;
.5 ensure searching the delivery vehicle; and
.6 ensure escorting delivery vehicles within the port facility.

16.38 For ships regularly using the port facility it may be appropriate to establish procedures involving the ship, its suppliers and the port facility covering notification and timing of deliveries and their documentation. There should always be some way of confirming that stores presented for delivery are accompanied by evidence that they have been ordered by the ship.

Security Level 1

16.39 At security level 1, the PFSP should establish the security measures to be applied to control the delivery of ship's stores, which may include:

.1 checking of ship's stores;
.2 advance notification as to composition of load, driver details and vehicle registration; and
.3 searching the delivery vehicle.

16.40 Checking of ship's stores may be accomplished by some or all of the following means:

.1 visual and physical examination; and
.2 using scanning/detection equipment, mechanical devices or dogs.

Security Level 2

16.41 At security level 2, the PFSP should establish the additional security measures to be applied to enhance the control of the delivery of ship's stores, which may include:

.1 detailed checking of ship's stores;
.2 detailed searches of the delivery vehicles;
.3 co-ordination with ship personnel to check the order against the delivery note prior to entry to the port facility; and
.4 escorting the delivery vehicle within the port facility.

16.42 Detailed checking of ship's stores may be accomplished by some or all of the following means:

.1 increasing the frequency and detail of searches of delivery vehicles;
.2 increasing the use of scanning/detection equipment, mechanical devices, or dogs; and
.3 restricting, or prohibiting, entry of stores that will not leave the port facility within a specified period.

Security Level 3

16.43 At security level 3, the port facility should ensure compliance with the instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility, in close co-operation with those responding and the ships at the port facility which may include preparation for restriction, or suspension, of the delivery of ship's stores within all, or part, of the port facility.

Handling Unaccompanied Baggage

16.44 The PFSP should establish the security measures to be applied to ensure that unaccompanied baggage (i.e. any baggage, including personal effects, which is not with the passenger or ship's personnel member at the point of inspection or search) is identified and subjected to appropriate screening, including searching, before is allowed in the port facility and, depending on the storage arrangements, before it is transferred between the port facility and the ship.
It is not envisaged that such baggage will be subjected to screening by both the port facility and the ship, and in cases where both are suitably equipped, the responsibility for screening should rest with the port facility.
Close co-operation with the ship is essential and steps should be taken to ensure that unaccompanied baggage is handled securely after screening.

Security Level 1

16.45 At security level 1, the PFSP should establish the security measures to be applied when handling unaccompanied baggage to ensure that all unaccompanied baggage is screened or searched up to and including 100 percent, which may include use of x-ray screening.

Security Level 2

16.46 At security level 2, the PFSP should establish the additional security measures to be applied when handling unaccompanied baggage which should include 100 percent x-ray screening of all unaccompanied baggage.

Security Level 3

16.47 At security level 3, the port facility should ensure compliance with the instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility, in close co-operation with those responding and the ships at the port facility, which may include:

.1 subjecting such baggage to more extensive screening, for example x-raying it from at least two different angles;
.2 preparations for restriction or suspension of handling or unaccompanied baggage; and
.3 refusal to accept unaccompanied baggage into the port facility.

Monitoring the Security of the Port Facility

16.48 The port facility should have the capability to monitor the port facility and its approaches, on land and water, at all times, including the night hours and periods of limited visibility, the restricted areas within the port facility, the ships at the port facility and areas surrounding ships. Such monitoring can include use of:

.1 lighting;
.2 security guards, including foot, vehicle and waterborne patrols, and
.3 automatic intrusion detection devices and surveillance equipment.

16.49 When used, automatic intrusion detection devices should activate an audible and/or visual alarm at a location that is continuously attended or monitored.

16.50 The PFSP should establish the procedures and equipment needed at each security level and the means of ensuring that monitoring equipment will be able to perform continually, including consideration of the possible effects of weather or of power disruptions.

Security Level 1

16.51 At security level 1, the PFSP should establish the security measures to be applied which may be a combination of lighting, security guards or use of security and surveillance equipment to allow port facility security personnel to:

.1 observe the general port facility area, including shore and water-side accesses to it;
.2 observe access points, barriers and restricted areas, and
.3 allow port facility security personnel to monitor areas and movements adjacent to ships using the port facility, including augmentation of lighting provided by the ship itself.

Security Level 2

16.52 At security level 2, the PFSP should establish the additional security measures to be applied to enhance the monitoring and surveillance capability, which may include:

.1 increasing the coverage and intensity of lighting and surveillance equipment, including the provision of additional lighting and surveillance coverage;
.2 increasing the frequency of foot, vehicle or waterborne patrols, and
.3 assigning additional security personnel to monitor and patrol.

Security Level 3

16.53 At security level 3, the port facility should ensure compliance with the instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility, in close co-operation with those responding and the ships at the port facility, which may include:

.1 switching on all lighting within, or illuminating the vicinity of, the port facility;
.2 switching on all surveillance equipment capable of recording activities within, or adjacent to, the port facility; and
.3 maximising the length of time such surveillance equipment can continue to record.

Differing Security Levels

16.54 The PFSP should establish details of the procedures and security measures the port facility could adopt if the port facility is at a lower security level than that applying to a ship.

Activities not covered by the Code

16.55 The PFSP should establish details of the procedures and security measures the port facility should apply when:

.1 it is interfacing with a ship which has been at a port of a State which not a Contracting Government;
.2 it is interfacing with a ship to which this Code does not apply; and
.3 it is interfacing with fixed or floating platforms.

Declarations of Security

16.56 The PFSP should establish the procedures to be followed when on the instructions of the Contracting Government the PFSO requests a Declaration of Security.

Audit, Review and Amendment

16.57 The PFSP should establish how the PFSO intends to audit the continued effectiveness of the PFSP and the procedure to be followed to review, update or amend the PFSP. The independence of any internal audit should be ensured.

16.58 The PFSP should be reviewed at the discretion of the PFSO. In addition it should be reviewed:

.1 if the PFSA relating to the port facility is altered;
.2 if an independent audit of the PFSP or the Contracting Government's testing of the port facility security organization identifies failings in the organization or questions the continuing relevance of significant element of the approved PFSP;
.3 following security incidents or threats thereof involving the port facility; and
.4 following changes in ownership or operational control of the port facility.

16.59 The PFSO can recommend appropriate amendments to the approved plan following any review of the plan. Amendments to the PFSP relating to:

.1 proposed changes which could fundamentally alter the approach adopted to maintaining the security of the port facility; and
.2 the removal, alteration or replacement of permanent barriers, security and surveillance equipment and systems etc., previously considered essential in maintaining the security of the port facility;

should be submitted to the Contracting Government that approved the original PSFP for their consideration and approval. Such approval can be given by, or on behalf of, the Contracting Government with, or without, amendments to the proposed changes.
On approval of the PFSP the Contracting Government should indicate which procedural or physical alterations have to be submitted to it for approval.

Approval of Port Facility Security Plans

16.60 PFSPs have to be approved by the relevant Contracting Government. Contracting Governments should establish appropriate procedures to provide for:

.1 the submission of PFSPs to them;
.2 the consideration of PFSPs;
.3 the approval of PFSPs, with or without amendments;
.4 consideration of amendments submitted after approval, and
.5 procedures for inspecting or auditing the continuing relevance of the approved PFSP.

At all stages steps should be taken to ensure that the contents of the PFSP remains confidential.

17 PORT FACILITY SECURITY OFFICER

Relevant guidance is provided under sections 15, 16 and 18.

18 TRAINING AND DRILLS

18.1 The Port Facility Security Officer should have knowledge and receive training**,** in some or all of the following, as appropriate:

.1 security administration;
.2 relevant international conventions, codes and recommendations;
.3 relevant Government legislation and regulations;
.4 responsibilities and functions of other security organisations;
.5 methodology of port facility security assessment;
.6 methods of ship and port facility security surveys and inspections;
.7 ship and port operations and conditions;
.8 ship and port facility security measures;
.9 emergency preparedness and response and contingency planning;
.10 instruction techniques for security training and education, including security measures and procedures;
.11 handling sensitive security related information and security related communications;
.12 knowledge of current security threats and patterns;
.13 recognition and detection of weapons, dangerous substances and devices;
.14 recognition of characteristics and behavioural patterns of persons who are likely to threaten the security;
.15 techniques used to circumvent security measures;
.16 security equipment and systems, and their operational limitations;
.17 methods of conducting audits, inspection, control and monitoring;
.18 methods of physical searches and non-intrusive inspections;
.19 security drills and exercises, including drills and exercises with ships; and
.20 assessment of security drills and exercises.

18.2 Port facility personnel having specific security duties should have knowledge and receive training**,** in some or all of the following, as appropriate:

.1 knowledge of current security threats and patterns;
.2 recognition and detection of weapons, dangerous substances and devices;
.3 recognition of characteristics and behavioural patterns of persons who are likely to threaten security;
.4 techniques used to circumvent security measures;
.5 crowd management and control techniques;
.6 security related communications;
.7 operations of security equipment and systems;
.8 testing, calibration and maintenance of security equipment and systems,
.9 inspection, control, and monitoring techniques; and
.10 methods of physical searches of persons, personal effects, baggage, cargo, and ship's stores.

18.3 All other port facility personnel should have knowledge and receive training**,** in some or all of the following, as appropriate:

.1 the meaning and the consequential requirements of the different security levels;
.2 recognition and detection of weapons, dangerous substances and devices;
.3 recognition of characteristics and behavioural patterns of persons who are likely to threaten the security; and
.4 techniques used to circumvent security measures.

18.4 The port facility should conduct frequent and detailed drills to ensure that port facility personnel are proficient in all assigned security duties for all security levels and to identify any security related deficiencies which need to be addressed.

19 VERIFICATION AND CERTIFICATION OF SHIPS

No additional guidance.

APPENDIX TO PART B

APPENDIX 1

DECLARATION OF SECURITY

Name of Ship:	
Port of Registry:	
IMO Number:	
Name of Port Facility:	

This Declaration of Security is valid from …….. until ……, for the following ship/port interface activities under Security Level ……..

……..
(list of the ship/port interface activities with relevant details)

The port facility and ship agree to the following security measures and responsibilities to ensure compliance with the requirements of Part A of the International Ship and Port Facility Security Code.

Activity	The port facility will: *(describe the arrangements)*	The ship will: *(describe the arrangements)*
Ensuring the performance of all security duties		
Monitoring restricted areas to ensure that only authorized personnel have access		
Controlling access to the port facility		
Controlling access to the ship		
Monitoring of the port facility, including berthing areas and areas surrounding the ship		
Monitoring of the ship, including berthing areas and areas surrounding the ship		
Handling of cargo		
Delivery of ship's stores		
Handling unattended baggage		
Controlling the embarkation of persons and their effects		
Ensuring that security communication is readily available between the ship and port facility		

The signatories to this agreement certify that security measures and arrangements for both the port facility and the ship during the specified ship/port interface activities meet the provisions of chapter XI-2 and Part A of Code.

Dated at ……..……on the ……

Signed for and on behalf of	
the port facility:	the ship:
(Signature of Port Facility Security Officer)	*(Signature of Master or Ship Security Officer)*

Name and title of person who signed	
Name:	Name:
Title :	Title :

Contact Details *(to be completed as appropriate)*	
for the port facility:	for the ship:
Port Facility	Master
Port Facility Security Officer	Ship Security Officer
	Company
	Company Security Officer